

FORM PTO-1390
(REV 12-29-99)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

**TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371**

PA1064US

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)

09/554417
UNKNOWNINTERNATIONAL APPLICATION NO.
PCT/US99/24088INTERNATIONAL FILING DATE
October 14, 1999PRIORITY DATE CLAIMED
October 14, 1998

TITLE OF INVENTION

System And Method Of Securing A Computer From Unauthorized Access

APPLICANT(S) FOR DO/EO/US

Lynn Spraggs

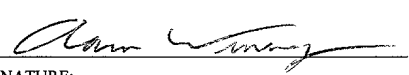
529 Rec'd PCT/PTO 11 MAY 2000

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C.371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ has been transmitted by the International Bureau.
 - c. ☒ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(3)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19(35 U.S.C. 371(c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A **FIRST** preliminary amendment.
☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: Verified Statement Claiming Small Entity Status;
Petition to Make Special Because of Prospective Manufacture Under 37 C.F.R. 1.102; Statement in Support of Petition to Make Special;
Petition Fee (\$130.00)

U.S. APPLICATION NO. (If known, 37 CFR 1.5) 007/354417		INTERNATIONAL APPLICATION NO. PCT/US99/24088		ATTORNEY'S DOCKET NUMBER PA1064US	
17. <input checked="" type="checkbox"/> The following fees are submitted: BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) : Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO \$970.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO \$840.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$690.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$670.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) \$96.00 ENTER APPROPRIATE BASIC FEE AMOUNT =				CALCULATIONS PTO USE ONLY	
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				\$	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	16 - 20 =	0	X \$18.00	\$	0.00
Independent claims	3 - 3 =	0	X \$78.00	\$	0.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ \$260.00	\$	0.00
TOTAL OF ABOVE CALCULATIONS =				\$	690.00
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).				\$	345.00
SUBTOTAL =				\$	345.00
Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$	0.00
TOTAL NATIONAL FEE =				\$	345.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property				\$	40.00
TOTAL FEES ENCLOSED =				\$	385.00
				Amount to be refunded:	\$
				charged:	\$
a. <input checked="" type="checkbox"/> A check in the amount of \$ <u>385.00</u> to cover the above fees is enclosed. b. <input type="checkbox"/> Please charge my Deposit Account No. _____ in the amount of \$ _____ to cover the above fees. A duplicate copy of this sheet is enclosed. c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <u>06-0600</u> . A duplicate copy of this sheet is enclosed.					
NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.					
SEND ALL CORRESPONDENCE TO: Aaron R. Wininger Carr & Ferrell, LLP 2225 East Bayshore Road, Suite 200 Palo Alto, CA 94303					
				 SIGNATURE:	
				<u>Aaron R. Wininger</u> NAME	
				<u>45,229</u> REGISTRATION NUMBER	

Atty. Dkt.No. PA1064US

Applicant: Lynn Spraggs
PCT International Serial No.: PCT/US99/24088
PCT Filed: October 14, 1999
US Serial No. Unknown
For: System and Method of Securing a Computer from Unauthorized Access

VERIFIED STATEMENT (DECLARATION) CLAIMING
SMALL ENTITY STATUS
(37 CFR 1.9 (f) and 1.27 (c)) - SMALL BUSINESS CONCERN

I hereby declare that I am:

- ☐ the owner of the small business concern identified below:
☒ an official of the small business concern empowered to
act on behalf of the concern identified below:

NAME OF CONCERN Aegis Systems Inc.
ADDRESS OF CONCERN 1101 San Antonio Road, Suite 409
Mountain View, CA 94043

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.2, and reproduced in 37 CFR 1.9 (d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled "System and Method of Securing a Computer from Unauthorized Access", by inventor Lynn Spraggs, as described in

- ☐ the specification filed herewith.
☒ PCT application serial no. PCT/US99/24088, filed October 14, 1999.
☐ patent no. _____, issued _____.

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e). *NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

NAME _____

ADDRESS _____

☐ INDIVIDUAL ☐ SMALL BUSINESS CONCERN ☐ NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28 (b))

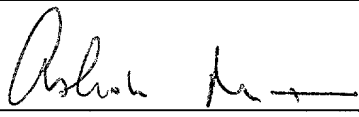
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of the Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING ASHOK MATHUR

TITLE OF PERSON IF OTHER THAN OWNER President

ADDRESS OF PERSON SIGNING 1101 San Antonio Road, Suite 409

Mountain View, CA 94043

SIGNATURE  DATE 4/27/00

SYSTEM AND METHOD OF SECURING A COMPUTER FROM
UNAUTHORIZED ACCESS

5

BACKGROUND OF THE INVENTION

1. Field of the invention

10 The present invention relates generally to computer security and more specifically to making a computer impervious to unwanted users and methods thereof.

2. Description of the Prior Art

15 In order to maintain a computer server on the Internet, the server generally needs to be secured so that unwanted users will not break into sensitive areas on the server, particularly if the server is being used as an e-commerce server. One way to protect the server is to screen incoming requests with a firewall.

20 A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Basically, a firewall filters all network packets to determine whether to forward them toward their destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources. However, a firewall is generally not impervious to unwanted users.

Since a firewall screens requests, the amount of traffic entering the server slows down considerably. Firewalls can be very complex and expensive, and often require an experienced technician to install and maintain. Furthermore, firewalls are open to attack from hackers, and once penetrated a hacker can gain supervisory rights to the server and access sensitive areas.

Thus, it would be desirable to provide a system and method of securing a computer that does not slow down traffic to the server, is easy to install, easy to use, inexpensive, and impervious to attack by unwanted users.

SUMMARY OF THE INVENTION

The present invention provides a system and method of securing a server computer from unauthorized access without requiring a firewall. The server computer is secured from an external client computer over the Internet or a network by removing the server's root or supervisor rights. The external client computer can be authorized through a trusted IP address list, as well as requiring a password key from the user of the external client computer. A telnet session and an ftp session can remain connected between the server computer and the Internet in order to manage the server computer while it is locked. Even though the supervisor rights have been removed from the server computer, an Internet session will continue to run to allow access to the server computer. The authorized external client can also restore the supervisor rights and manage the web server computer accordingly.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying illustrations. For
5 simplicity and ease of understanding, common numbering of elements is employed where an element is the same in different illustrations.

FIG. 1 is a schematic diagram illustrating a client requesting
10 access to a secure server over the Internet, in accordance with the present invention;

FIG. 2 is a block diagram of the secure server computer shown
15 in FIG. 1, in accordance with the present invention;

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module located within the secure server computer of FIG. 2;
and

20 FIG. 4 is a flowchart of a method illustrating how an administrator can manage and secure the server computer, according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The following is a detailed description of illustrative embodiments of the present invention. As these embodiments of the present invention are described with reference to the aforementioned illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

Referring now to FIG. 1, a schematic diagram illustrates a web server 100 and a client computer 102 connected to the Internet 104. Excellent results can be obtained when the web server 100 is running a Unix® operating system, however, other operating systems such as Windows® can also be used. A qualified user or an administrator using a client computer 102 has the ability to access the server 100 through the Internet 104 in order to manage the server 100 and to pseudo lock the server 100 so that no unauthorized access can be gained.

FIG. 2 is a block diagram of the web server computer 100 shown in FIG. 1. Computer 100 includes a CPU 202, RAM 204, non-volatile memory 206, an input device 208, a display 210, and an Internet interface 212 for providing access to the Internet.

5 FIG. 3 is a block diagram of one embodiment of the non-volatile memory module 206 located within the web server computer 100 of FIG. 2. The non-volatile memory 206 includes a database of secure keys 302, a listing of trusted IP addresses 304, and an access engine 306. The database of secure keys 302 includes at least one
10 authorized key or password that is known or held by the server administrator. The access engine 306 provides the administrator with various features for managing the web server computer 100, these features include: a remove supervisor rights engine 308, a restore supervisor rights engine 310, and management tools 312.

15 During the initial installation of the access engine 306 a password or a secure key 302 is established by the server administrator. The access engine 306 is programmed so that it is only accessible from an external client computer having a trusted IP address. The administrator is able to specify IP addresses that would
20 allow access to the access engine 306.

FIG. 4 is a flowchart of a method illustrating how to secure and manage the web server computer from an authorized client computer through the Internet in accordance with the invention. The administrator begins his request for access to the web server

computer from a client computer at step 400 by starting the access engine. Next at step 402 it is determined if the request from the client computer is from a trusted IP address. The web server computer checks to see if the IP address of the requesting client computer is in the list of trusted IP addresses 304.

If the IP address of the requesting client is not in the list of trusted IP addresses 304 then at step 404 the client request to manage the web server computer is rejected. If the IP address of the requesting client is found in the listing of trusted IP addresses 304, then at step 406 a key or password is requested from the client. It is possible for computer hackers to "spoof" an IP address from an untrusted IP address, therefore an additional security measure of requiring a password is provided for a higher level of security.

If the password entered from the client is not in the database of secure keys 302 then at step 404 the client request to manage the web server computer is rejected. If the key entered from the client is in the database of secure keys 302, then the requesting client is authorized to manage the web server computer.

After being authorized to manage the web server computer, at step 410 the administrator decides whether to lock the server. If the administrator decides to lock the server then at step 412 supervisor rights on the web server computer are then physically removed thereby locking the server computer from any unauthorized access, and at step 424 the process ends. Prior to removing the supervisor

rights on the web server, a telnet session and an ftp session are established with the web server so that the web server can still be accessed over the Internet by, and only by, the client 102.

In order to lock the server, the root, or alias root, is physically removed from the server. This requires rewriting the password file without any supervisory rights in it. In a UNIX operating system, in order to physically remove the root or the supervisory rights from the server, the User ID = 0 (UID=0) and the Group ID = 0 (GID=0) are removed from the computer's user list and group list. After the root is removed, the web server computer is functionally dead or secure and no supervisory commands can be issued at the console of the web server, but the telnet session and the ftp session stay connected and allow the trusted client to access the server over the Internet. Even though the server is functionally dead and nobody can access the server as a supervisor, other applications on the web server continue to run and allow access from users on the Internet.

If, at step 410, the administrator does not lock the server, then at step 414 the administrator has the option to unlock the web server if the server has been previously locked. If the administrator chooses to unlock the server then at step 416 supervisor rights on the server are restored, and at step 424 the process ends. In order to restore the supervisor rights, the supervisor is added to the user list and the group list (i.e. UID=0 and GID=0 is added).

If, at step 414, the server is not unlocked, then at step 418 the administrator can choose to process other requests, such as managing the files on the server. At step 420 any requests by the administrator from the trusted client are processed, and at step 424 the process then ends. If no requests are made by the administrator, then at step 422 the access engine goes through error processing and at step 424 the process ends.

I Claim:

- 1 1. A system for securing a server computer from unauthorized
2 access, comprising:
3 an access engine for removing supervisor rights on the server
4 computer.
- 1 2. The system of claim 1, wherein removing supervisor rights
2 includes removing a root from the server.
- 1 3. The system of claim 1, wherein the access engine allows
2 removing supervisor rights from an external client computer.
- 1 4. The system of claim 3, wherein the access engine allows
2 supervisor rights to be restored on the server computer from an
3 external client computer.
- 1 5. The system of claim 3, further including a list of trusted IP
2 addresses, wherein the external client computer can only remove
3 supervisor rights on the server computer if the external client
4 computer has an IP address in the list of trusted IP addresses.

1 6. The system of claim 5, further including a password key,
2 wherein the external client computer can only remove supervisor
3 rights on the server computer if the password key is provided by a
4 user of the external client computer.

1 7. The system of claim 1, wherein the server computer is a world-
2 wide-web server computer connected to an Internet.

1 8. A method of securing a server computer from unauthorized
2 access, comprising the steps of:
3 removing supervisor rights on the server computer; and
4 allowing external access to applications on the server computer.

1 9. The method of claim 8, further including the steps of:
2 providing a list of trusted IP addresses; and
3 authorizing an external client computer to remove supervisor
4 rights only if the external client computer has an IP address in the list
5 of trusted IP addresses.

1 10. The method of claim 9, further including the steps of:
2 providing a password key; and
3 authorizing the external client computer to remove supervisor
4 rights only if the password key is provided by a user of the external
5 client computer.

1 11. The method of claim 8, wherein removing supervisor rights
2 includes removing a root from the server computer.

1 12. The method of claim 8, wherein removing supervisor rights can
2 be done from an external client computer over an internet.

1 13. A computer-readable medium comprising program instructions
2 for securing a server computer from unauthorized access, by
3 performing the steps of:
4 removing supervisor rights on the server computer from an
5 external client computer; and
6 allowing external access to applications on the server computer.

1 14. The computer-readable medium of claim 13, further performing
2 the steps of:
3 providing a list of trusted IP addresses; and
4 authorizing the external client computer to remove supervisor
5 rights only if the external client computer has an IP address in the list
6 of trusted IP addresses.

1 15. The computer-readable medium of claim 14, further performing
2 the steps of:
3 providing a password key; and
4 authorizing the external client computer to remove supervisor
5 rights only if the password key is provided by a user of the external
6 client computer.

1 16. The computer-readable medium of claim 13, wherein removing
2 supervisor rights includes removing a root from the server computer.

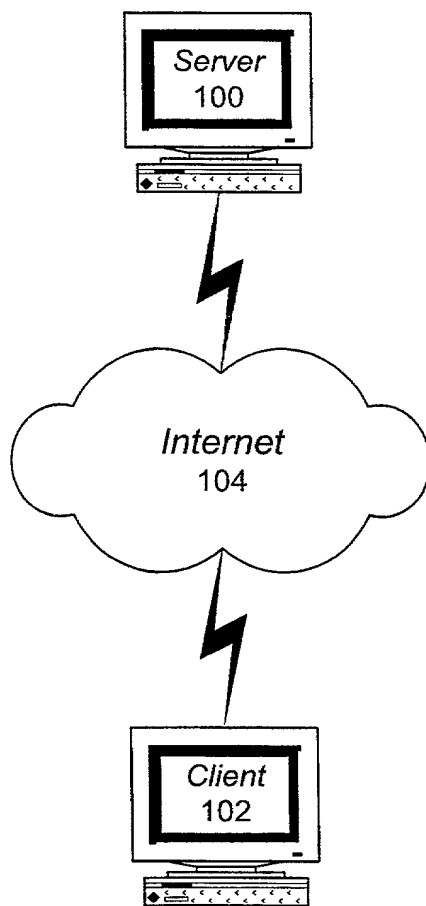
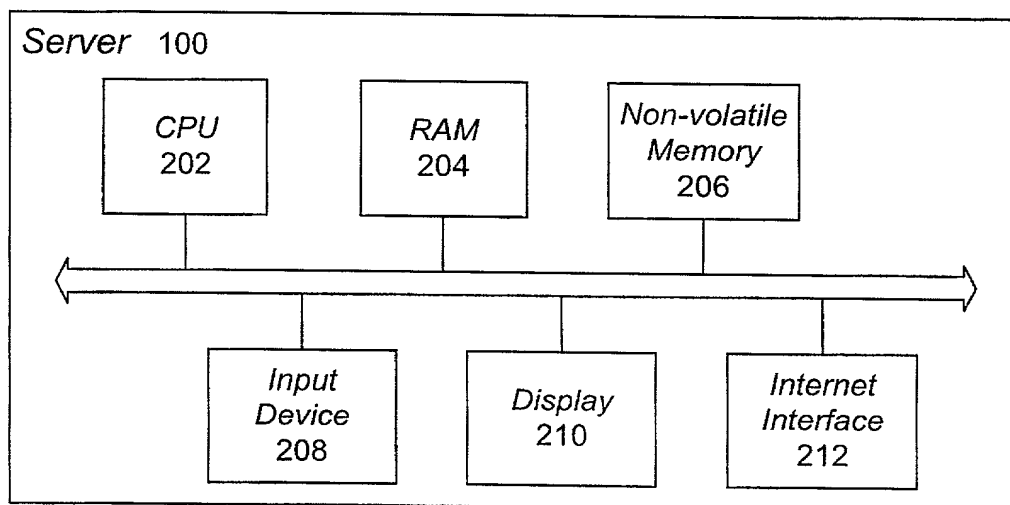
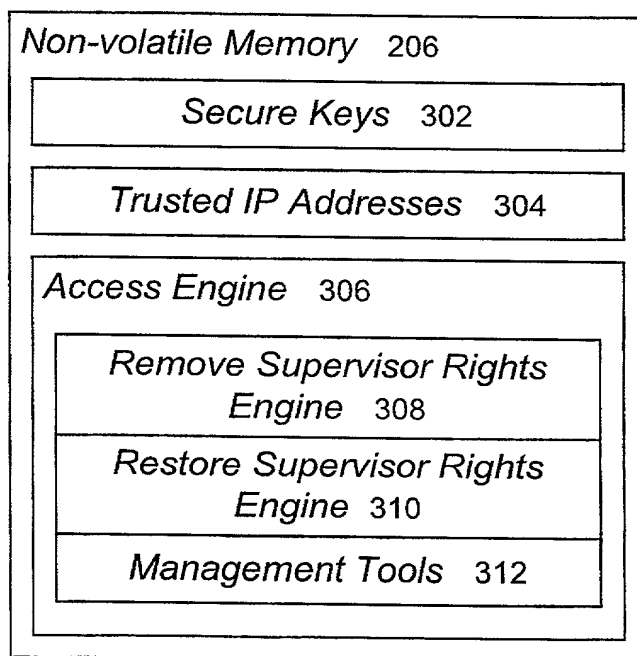
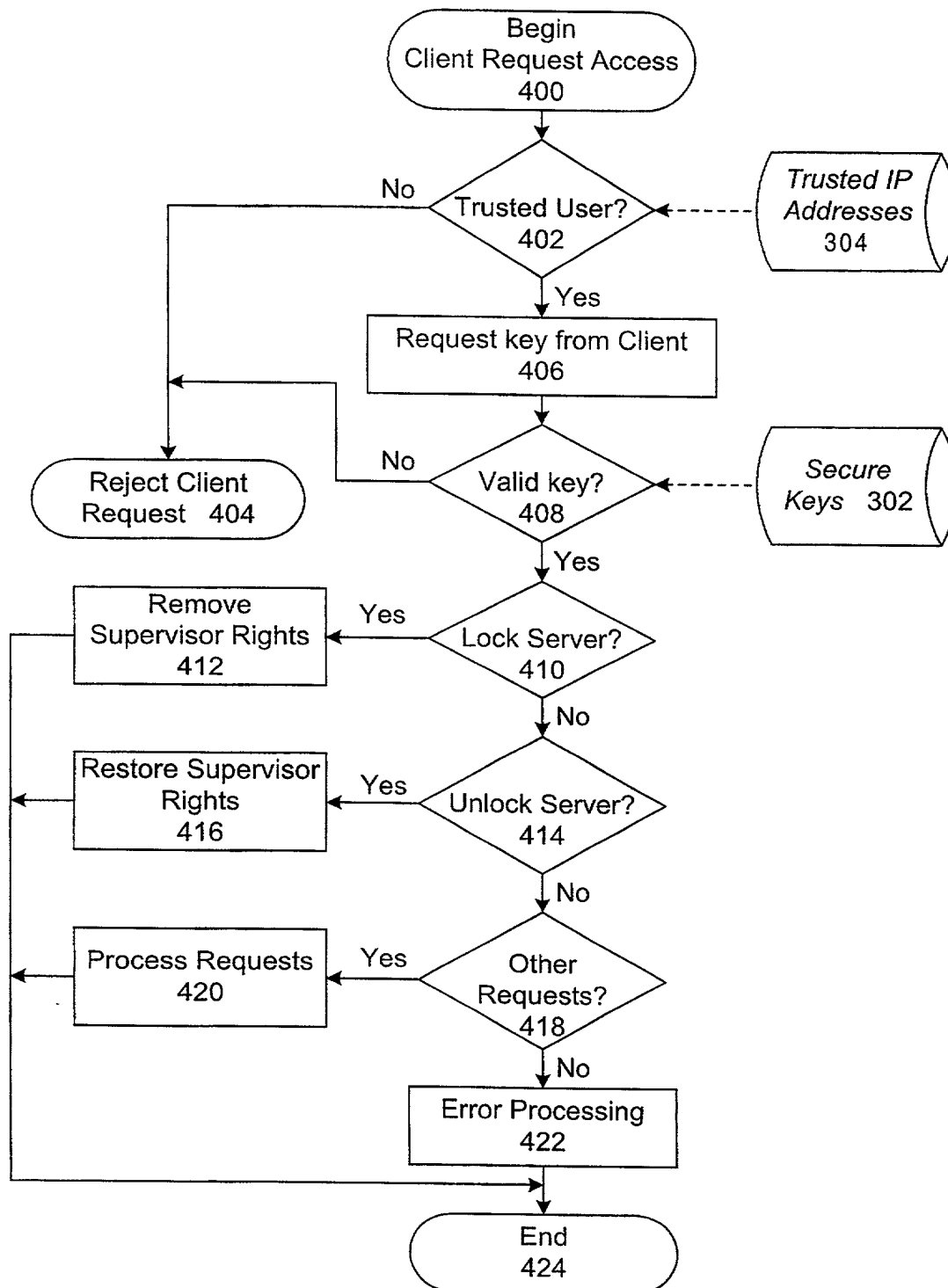


FIG. 1

**FIG. 2****FIG. 3**

3/3

**FIG. 4**

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled "**System and Method of Securing a Computer From Unauthorized Access,**" the specification of which (check one):

☐ is attached hereto.

☒ was filed on October 14, 1999
as U.S. Application No. _____
or PCT International Application No. PCT/US99/24088
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Claimed

_____ (Number)	_____ (Country)	_____ (Day/Month/Year filed)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year filed)	<input type="checkbox"/> Yes	<input type="checkbox"/> No

I hereby claim the benefit under Title 35, United States Code §119(e) of any United States provisional application(s) listed below.

(Application Number)

(Filing Date)

(Application Number)

(Filing Date)

I hereby claim the benefit under Title 35, United States Code §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

PCT/US99/24088

October 14, 1999

Pending

(Application Number)

(Filing Date)

(Status -- patented, pending, abandoned)

(Application Number)

(Filing Date)

(Status -- patented, pending, abandoned)

POWER OF ATTORNEY: I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

8

John S. Ferrell, Reg. No. 34,593; J. Eppa Hite, Reg. No. 30,266;
Gregory J. Koerner, Reg. No. 38,519; Charles B. Katz, Reg. No. 36,564;
John D. Henkhaus, Reg. No. 42,656; Susan Yee, Reg. No. 41,388;
Robert Toczycki, Reg. No. 38,341 and Aaron Wininger, Reg. No. 45,229.

SEND ALL CORRESPONDENCE TO:

Aaron Wininger
CARR & FERRELL LLP
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303
TEL: (650) 812-3400
FAX: (650) 812-3444

0005 Y/V

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole inventor: Lynn Spraggs

Inventor's signature [Signature] Dated: 3/28/2000

Residence 8604 Kalavista Dr

Post Office Address Vernon B.C. Canada ^{CAN} Citizenship Canadian